On the importance of securing telephony systems

IOSIF I. ANDROULIDAKIS
Network Operations Center
University of Ioannina
Dourouti Campus, Ioannina, GR45110
GREECE
sandro@noc.uoi.gr

Abstract—In the following work we present an easy to read essay about the array of threats that modern telephony systems face, that will prove, hopefully, useful for both administrators and simple users. We have taxonomized these threats and we have further provided some useful tips for safeguarding these systems in order to keep enjoying one of the most valuable goods: That of communication.

Key-Words: Telephony Threats, Telephony Fraud, Communication Systems Security

1. Introduction

"It is not a matter of if; it is a matter of when". Most of us have come across that saying, regarding a computer or network incident. Many articles have been written to alert users and help administrators deal with the problems and much work has been carried out to safeguard the computing and network infrastructure [13]. But what about our plain old telephone? Can you recall any information regarding the classical telephony threats?

There are many issues concerning the threats telephony faces. We tried to address some of the basic problems that exist and threaten the telephones' security. We taxonomized them in an easy to read essay that will prove, hopefully, useful for both administrators and simple users. Our analysis is mainly focused on Private Branch Exchanges (PBXs). A PBX is a telephone exchange serving an individual organization or company with connections to the PSTN (Public Switched Telephone Network) [9].

PBXs make connections among the internal telephones of a private organization — usually a business — and also connect them to the public switched telephone network (PSTN) via trunk lines. It is actually a private switch or router that connects a group of telephones and provides a wealth of features. It is because they incorporate telephones, fax machines, modems, and more, that the general term "extension" is used to refer to any end point on the branch. A typical PBX is depicted in figure 1.

Initially, the primary advantage of PBXs was cost savings on internal phone calls: handling the circuit switching locally reduced charges for local phone service. As PBXs gained popularity, they started offering services that were not available in the operator network, such as hunt groups, call forwarding, and extension dialling.

With such an array of services and cost savings it is of no wander that there are millions of PBX lines installed in every country. PBXs essentially complement the public network. Even if the core public network is operating normally, unintentional or targeted damages and attacks in PBXs can cause significant instability and problems. Furthermore interception of calls is a very sensitive issue that affects all of us.

Fig. 1, A typical PBX

2. Problem Formulation

Contemporary societies rely on telecommunication infrastructure more than ever. Economy, Health, Industry, Security, private and public sector have extended telecommunication networks to serve their communication needs. Organizations, Ministries, Public bodies, Hospitals, Companies, Factories etc have their own telephone exchanges, based on PBXs. In that sense, it is not an exaggeration to state that PBXs are part of a nation's critical infrastructure.

As telephony security is usually lacking compared to IT security, the opportunities for crime are numerous. The first thing that comes into mind is of course unauthorized access of our telephones and the relevant results. Losses due to computer incidents are usually estimated and it is indeed a very complex procedure yielding wrong results many times. Economic losses due to a telephony incident on the other hand are immediately obvious.

Imagine a telephony fraud taking place unnoticed for a substantial period. A month later the phone bills usually arrive in a box rather than in an envelope. Apart from the apparent cost of the bill, lost revenues and additional expenses can skyrocket the total loss to astronomical amounts.

Interception is also a well justified fear regarding the dangers that a compromised PBX poses to its owner. An attacker could intercept phone calls and logs getting valuable information and secrets. Apart from phone voice calls, fax calls or even low speed modem data communications can be intercepted and extracted with needles to comment consequences.

It is frightening to imagine not being able to call a hospital in an emergency. Furthermore, national economy could suffer great losses if a targeted attack was to render useless industry's telecommunication lines. In any case, it is apparent that in the modern demanding business environment a company or organization can't survive without telephone service. Even worse, consequences after a multimillion fraud starting from its own telephone exchange would lead to financial and business disaster.

2.1 Frauds and Fraudsters

Telecommunication fraudsters fall into three basic groups: those who do it for fun, those who do it to save money and those who do it for profit [2]. The scale of importance grows from low to extremely high, as Figure 2 shows. At the lower end of the impact scale are skilled individuals, usually teenagers trying to break in just for the challenge. The most common threat to a network is the malicious hacker who is usually trying to earn personal benefits by employing his skills in network management and programming to deploy various illegal activities such as call sell operations using stolen codes and accesses. Hackers often form Hacker Teams or groups to share their findings. He could also intercept phone calls and logs providing valuable information, especially in cases of industrial spying.

A common use of a compromised telephone network is to use it as a screen for covering-up criminal's illegal activities such as ring operations, drug selling, money laundry etc. The call usually originates from payphones because they can offer anonymity and they are easy to find and accessible from almost everywhere. Then the call is routed through many private telephone branch exchanges (PBXs) to make it extremely difficult to trace. This "looping" is a very effective way to mislead authorities from tracing them. The technique however, is on the decline with the advent of convenient prepaid mobile phones [3].

Organized crime has its own customer base that demands cheap international calls and will break into PBXs to serve this base. Knowing that the window of opportunity will close eventually they try to maximize their revenue by exploiting quickly and aggressively the compromised PBX [2]. Selling calls to high cost international destinations is the most usual fraud taking place. The unsuspected administrator who has not properly secured his PBX will face a very unpleasant surprise.

Fig. 2, List of importance of attackers

Spies have also lots to gain from intruding into PBXs. They can intercept valuable information, financial and technical data. In same cases, even just the call logs and not the conversation itself can reveal interesting secrets, such as the launch of a new product into the market.

At the other end of the spectrum are terrorists who according to recent surveys seem to manipulate telephone exchanges in order to raise funds for their purposes [16].

Typical methods of abuse by malicious hackers involve the misuse of common PBX functions such as DISA (Direct Inwards System Access), call forwarding, voicemail and auto attendant features. DISA is designed to allow remote users to access a PBX to place log distance calls as if they were at the same site as the PBX. Fraudsters unfortunately are another category of remote users. Voicemail use poses two possible threats. One is that if wrongly configured, they can give access to dial tone in order to place a call. The second one is the inherent dangers of stealing the information contained in them or even taking them over [10].

Wireless calls can passively be intercepted using the proper gear. A classical way of interception is the use of special devices, the well known "bugs". A more elaborate technique is that of "the man in the middle". In order to intercept a wireless communication a hacker can intervene in the middle pretending to be the other party and relaying the information to the intended party. That is why revealing sensitive information during a phone call is not a good idea unless some sort of cryptographic means is used.

Another sensitive point in a company's telephone network consists of the internal phones placed in publicly accessed areas (i.e in the lobby or in the elevator). As a matter of fact there is also a whole category in relevant articles in underground electronic magazines regarding what is called "elevator phreaking". Such phones are easy to access and as an internal part of the network can easily be misused to expose vulnerabilities. Internal phones are furthermore a great access point for all those who mean to cause harm to the network and its infrastructure. A person can easily slip a "bug" or use them just to place a free call. So they have to be both protected and confined in places that not everyone has access to them. In case they are really needed any necessary steps must be taken in order to secure them and make sure that they cannot cause problems.

A special case of an internal phone is the operator's console (Figure 3). If not properly administered, it may have the ability to change setup features and operational data. It could for example unblock barred destinations or leverage call abilities on certain phones.

Fig. 3, A typical PBX operator's console

Modern telephone exchanges use expensive and easily removed and carried equipment (i.e. exchange cards – boards, Figure 4) so a couple of minutes would be enough for an incident to take place causing apart from the economic damage also an outage.

Fig. 4, A typical PBX board

To make things worse, a dialup line connecting the telephone exchange's CPU to the maintainer's modem in order to remotely administer the switch can be misused causing not only telephone problems but also providing a way to enter the computer network. The Maintenance Port [10] as it is called, is usually protected with a simple to guess or default password making it easy to defeat. Having access to the switch, the hacker can reprogram it, turn on functions such as DISA and

shut down other functions such as call logging. It is interesting to note that call detail records contain a wealth of information as seen in Figure 5 PBXs are usually programmed using menu driven programs such as in Figure 6.

```
----[/DHS3dyn/account/TAXATGHP.DAT : Ticket number 6/6/6]----------
(00)           TicketVersion = ED5.1
(01)            CalledNumber = [redacted]
(02)           ChargedNumber = [redacted]
(03)         ChargedUserName = [redacted]
(04)       ChargedCostCenter = [redacted]
(05)          ChargedCompany =
(06)        ChargedPartyNode = 105
(07)              Subaddress =
(08)           CallingNumber =
(09)               CallType = PublicNetworkIncomingCallToPrivateNetwork
(10)               CostType = ISDNCircuitSwitchedCall
(11)            EndDateTime = 20080826 01:35:40
(12)            ChargeUnits = 0
(13)               CostInfo = 0
(14)               Duration = 417
(15)          TrunkIdentity = 360
(16)      TrunkGroupIdentity = 1
(17)               TrunkNode = 101
(18)      PersonalOrBusiness = Normal
(19)              AccessCode =
(20)      SpecificChargeInfo =
(21)        BearerCapability = Speech
(22)           HighLevelComp = Unspecified
(23)              DataVolume = 0
(24)        UserToUserVolume = 0
(25)        ExternFacilities =
(26)        InternFacilities = BasicCall
(27)           CallReference = 0
(28)           SegmentsRate1 = 0
(29)           SegmentsRate2 = 0
(30)           SegmentsRate3 = 0
(31)                 ComType = Voice
(32)     X25IncomingFlowRate = Unspecified
(33)     X25OutgoingFlowRate = Unspecified
(34)                 Carrier = 0
(35)    InitialDialledNumber = [redacted]
(36)         WaitingDuration = 1
(37)   EffectiveCallDuration = 417
(38)  RedirectedCallIndicator = 0
(39)           StartDateTime = 20080826 01:28:43
(40)   ActingExtensionNumber =
(41)        CalledNumberNode = 9999
(42)       CallingNumberNode = 9999
(43) InitialDialledNumberNode = 9999
(44) ActingExtensionNumberNode = 9999
(45) TransitTrunkGroupIdentity = 32767
(46)          NodeTimeOffset = 0
```

Fig. 5, A typical PBX call detail record

There is a well known technique, called "war dialing" which consists of calling every single number a company owns in order to discover modems and electronic services to abuse. According to a recent survey [11] regarding information security controls, "testing and review procedures including a "war dial" of inbound phone lines to identify active modems" ranked last in a list of 80 controls. In other words, the identification and tracking of modem connections was incomplete, of low quality and not rationalized posing a significant risk that shouldn't be neglected. Our experimental survey among 100 PBXs which follows in section 2.3 confirmed these findings and revealed further statistical data.

```
Select an object

    Shelf
    Media Gateway
    PWT/DECT System
    System
    Translator
    Classes of Service
    Attendant
=>  Users
    Users by profile
    Set Profile
    Groups
    Speed Dialing
    Phone Book
    Entities
    Trunk Groups
    External Services
    Inter-Node Links
    X25
    DATA
    Applications
    Specific Telephone Services
    ATM
    Events Routing Discriminator
    Security and Access Control
    IP
    SIP
    DHCP Configuration
    Alcatel-Lucent 8&9 Series
    Encryption
    Passive Com. Server
    SNMP Configuration
```

Fig. 6, Menu driven PBX programming

When a PBX is linked to an organization's IT network as in Figure 7, a poorly protected maintenance port can offer an open and undefended "back door" into such critical assets as customer databases and business applications [1]. Imagine a fraudster, having the ability to intercept credit card numbers as the unsuspected client presses the keys in his phone [3]. There are many cases where a perfectly well designed computer network is brought down due to errors and omissions in the telephone network. It is rather oxymoron to invest into computer security but to forget to invest into telephone security. Total security can only be

achieved with combined efforts and supplies between IT and telecom world.

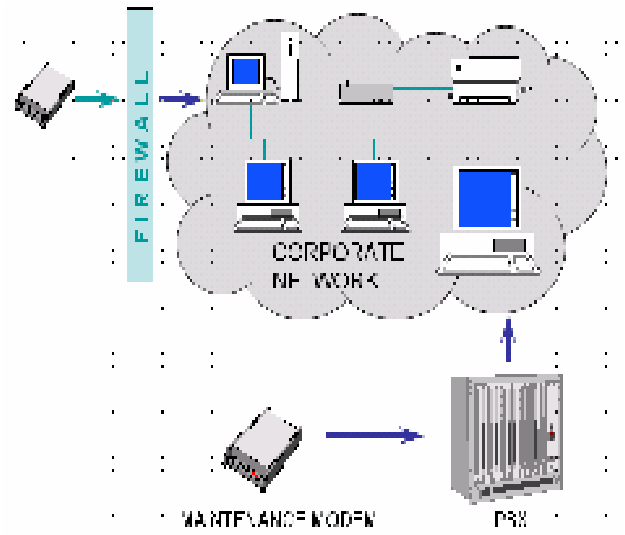

Fig. 7, Firewall bypass due to maintenance modem

Most administrators use firewalls and check their computer network's health regularly. Unfortunately the telephone network can help breach the firewall protection. All it takes is an unauthorized modem hooked up in an internal line and presto! Access to Internet is now possible and viruses and trojan horses lurking can now find their way in through an unguarded entry point.

Apart from fraud and interception, another hit in our infrastructure can come from what is called "denial of service" which is caused either intentionally or unintentionally and severely harms the integrity of our network especially if we don't have alternative routes or backup lines for our connections. In simple words, we cannot use our telephone to place or receive calls since it is no more operating. A company short on ethics could hire somebody to sabotage the telephone exchange of their competitor making it impossible to do business and causing huge losses. Finally a disgruntled former employer with a disordered sense of amusement could render such a telephone exchange useless in order to take revenge.

So far we have examined technical threats. However, it is not always necessary to be technically savvy to abuse a telephone network. A very common technique for accessing it is the use of Social Engineering; people who pretend to be someone else use their persuasion to extract valuable information for the network itself or information that can be helpful for infiltrating it. There are two good examples here, one is the use of Social Engineering by a person that impersonates a trusted one (i.e. an employee) via the phone and extracts information from a secretary, a username and a password to login to the network and the other is a person that gives false information and impersonates a network technician in order to extract information about the whereabouts of the PBX and take the secretaries approval to access it, and from there to have full access to the network. Further examples can be found in [4].

Closing our analysis we will move from threats coming from outside to threats that originate form the inside. Insiders are probably the most difficult enemy to deal with. They can prove a valuable ally for a hacker, providing him with passwords and information about the infrastructure. They could also simply give him permission to enter a company and poke around the equipment. Finally insiders could act by themselves exploiting our assets, planting "bugs" etc. For example, an employee, contractor or even a cleaner could forward a seldom-used extension to an overseas number and make international calls by calling a local rate number in the office. Needless to say who is actually paying the bill

2.2 The modus operandi

The modus operandi of a hacker and the sequence of actions attacking a PBX would be the following:

a) Pick up the target (either a specific one or a random one)

b) Do a thorough search in the yellow pages and in the internet for documented lines (directory of phones, direct dial in lines, etc.)

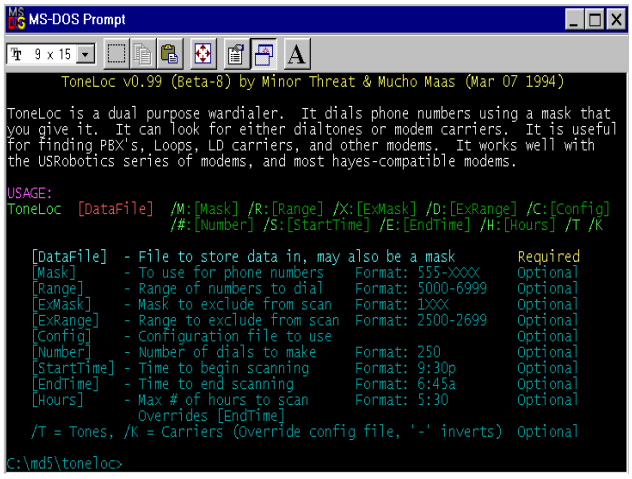

Fig. 8, DOS era war dialing program

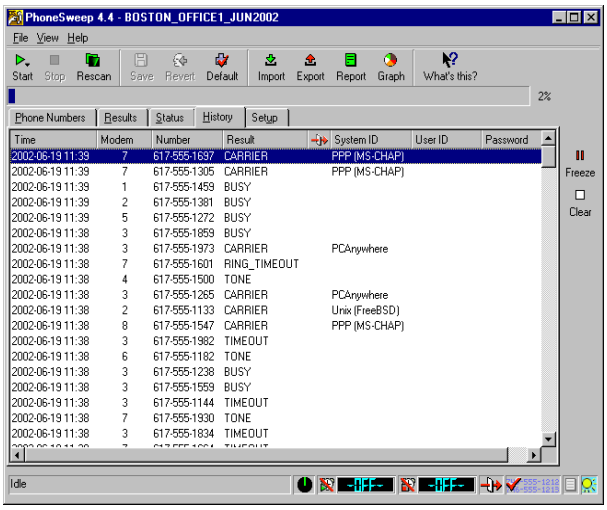

Fig. 9, Graphical user interface war dialing program

c) Proceed to war dialing, dialing all of the numbers in the specific numbering plan. This step is usually performed with automated tools (from DOS era – Figure 8 or using present GUI Operating Systems – Figure 9) but can be accomplished with manual dialing too. A simple spreadsheet sheet as in Figure 10 can be used in order to note down the details.

d) Judging by the tone and the pattern of the ring tone it might be possible to determine the type of the PBX. Most of the times, the music on hold theme is a clear indication of the PBX manufacturer.

e) When a modem is found then its prompt can help evaluate the type of the equipment connected. It might be a server, the PBX maintenance port, or an employee's PC. The hacker will proceed relevantly.

f) Should the PBX maintenance modem is found, then the default passwords would be the first ones to try. Otherwise guessing can have some success, while social engineering would probably also work. The login screen is usually identifying the concerned system (Figure 11).

g) Once inside the system, the attacker will initially deactivate logging features. He will then proceed to probing the system in order to understand its configuration. It is then relatively easy to create virtual numbers, to activate features such as DISA or immediate forward to premium rate service numbers, to download call records and do whatever he pleases. Furthermore, systems tend to be user friendly which is not always a good idea. In our case even if he does not know the exact arguments for the needed commands, an online help system, invoked by typing help or special characters such as "?" could help him.

h) If a service is found (DISA, Voice Mail, IVR) then it can also reveal information about the type of the PBX. Furthermore, each type has documented features and problems that the hacker might try to exploit.

i) Daring enough hackers could also physically present themselves to the PBX site, posing as technicians and asking to visit the PBX itself in order to proceed to "maintenance" works.

The previous steps can be assisted by social engineering tricks where the hacker will manipulate the human element in order to divulge valuable information as already mentioned before.

ABCD	0	1	2	3	4	5	6	7	8	9
00										
01										
02										
03										
04										
05										
06										
07										
08										
09										
10										
11										
12										
13										
14										
15										
16										
17										
...										
...										
...										
...										
...										
...										
...										
...										
80										
81										
82										
83										
84										
85										
86										
87										
88										
89										
90										
91										
92										
93										
94										
95										
96										
97										
98										
99										

Fig. 10, Manual war dialling matrix

Alongside the previous modus operandi, there is also the possibility to engage into a denial of service attack. Apart from obvious methods such as shutting down the PBX or stealing vital parts of it (such as the CPU), there are also less apparent techniques. One would be to instruct an array of different PBXs

to start calling the numbers of the victim PBX. It would overwhelm it with so many calls that legitimate users would not be able to access it. Inserting deliberate faults (i.e in the routing tables) and degradation of the PBXs capabilities (probably by reducing the number of available trunk lines) can also cause significant problems to the operation of the targeted company or organization.

2.3 Experimental data

In order to establish some experimental data regarding this process, the following experiment took place. The author located 100 organizations, companies, institutes, etc, in the yellow pages and tried to find their modem port. The war dialling process was limited to only 20 of the most probable numbers. These are numbers that end in XX (same digits) or have an ABCDXYZ form where XY or YZ are either AB, or BC, or CD.

Fig. 11, Login screen of a PBX

Out of the 100 organizations it was possible to find 67 maintenance modems, 12 out of them had the maintenance port in extension XXXX999, while 42 of them had the maintenance port located in extension XXXXX99. This means that after locating the PBX's main number (the directory number published in yellow pages) the hacker does' not even have to take step c).

After locating its target, an attacker can immediately dial extension 999 or 99 with the following results: If the PBX has at most 100 numbers then he has 70% chance of hitting the modem at once dialing XXXXX99! Otherwise, if the PBX has at most 1000 numbers then he has a 18% chance of hitting the modem dialing XXXX999. Other modem favourite numbers are: XXXX599 with 10% possibility, XXXX499, XXXX599 and XXXX899 with 6% possibility, XXXXX00 and XXXXX11, each with a 5% possibility.

3. Problem Solution

While data communications have long before begun to utilize every possible means of protection, enjoying a vivid research and development sector, PBX arena has not caught up. As a matter of fact, due to the much higher life expectancy and rigidity of PBXs it is common to find still operating more than 20 years old equipment. It is clear that a combined and targeted action has to be taken.

It might seem so far that we are left unable to defend our selves against the evil. This is not the case. There are many simple steps a savvy administrator can take to shield the PBX [7, 12], starting from proper education of the users and himself in order to increase the awareness of the system's security features and vulnerabilities. Education and properly enforced security procedures and policies can also help mitigate the danger of social engineering.

Properly communicated security policies should follow. Technical measures such as frequent system passwords changing, barring of premium rate calls, careful assignment of station privileges etc. can only be effective as soon as the users are educated. Manuals, directories and other internal documents should be treated as confidential. Call logging should always be enabled and checked for unusual activity and strange call patterns.

Furthermore, call forwarding to external destinations should not be allowed. Especially regarding maintenance port, every serial port connection should be traced to its destination. The modem should be switched on only when the maintainer needs to perform some action and with a well defined time schedule.

Dangerous features such as DISA and voicemail deserve also special attention. It is better to be disabled or even removed if they are of no use. Otherwise, in collaboration of the manufacturer, every suggested measure, patch and upgrade should be applied.

During the past few years an analogy of computer firewalls has made it into the telecommunication world. These PBX firewalls are connected between the PBX and the network and effectively control the parameters of each call. Should a call deviate from the normal call pattern (being too long, or headed towards a new destination, or taking place out of business hours etc) then it is logged or disconnected. Furthermore such a solution hosted in an isolated system solves the problem of breaching its integrity. The arrangement of this system is shown in Figure 12 (after [17]).

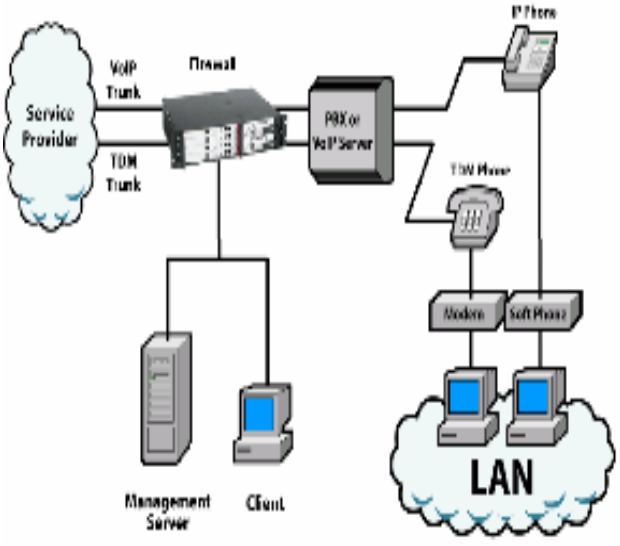

Fig. 12, PBX Firewall

Another technical solution, stemming from the banking experience uses a two factor authentication where the user has also to enter a random number produced by a token device. So apart from the password the user has also to respond to the challenge question, as seen in Figure 13.

The physical infrastructure and especially the expensive one should be protected with proper security measures, be kept in a controlled environment not easily accessible to everyone, and be well hidden from people that don't need to know where it is. A biometric authentication access system could also be considered, as proposed in [15]. In many companies, everyone is invited to have a look at their expensive PBX (Private Branch Exchange), which is waiting behind an open door. Just follow the signs that lead to the place. As a matter of fact many companies tend to advertise their "treasures" by signs and labels making it easier for the determined one to find.

```
CONNECT 38400

Login:
Login: [redacted]
Password:
INCORRECT LOGIN

Login: [redacted]
Password:
INCORRECT LOGIN

Login: [redacted]
Challenge: 5[redacted]63      Product ID: 1[redacted]

Response:
INCORRECT LOGIN
```

Fig. 13, Login and Challenge procedure

Furthermore protection from unauthorized access is a must because access to the premises means complete access to our network. A "bug" or other intercept device could be planted there, at the heart of our network.

Another usually forgotten aspect is the protection against environmental elements and disasters. A fire could burn our infrastructure endangering human lives too. A flood could prove extremely harmful for the sensitive and expensive equipment while a water pipe leak can cause a severe damage and a complete collapse of the network which will not be easy to deal with. It is of great importance to take all the appropriate measures to guard against such incidents. In case of a natural disaster, such as an earthquake, there

should always be provision for disaster recovery procedures.

Besides technical means, common sense and tidiness can help a lot. Equipment, patching and connections should be well documented not only to help technicians in their job to easily expand and service the network but also to make it possible to easily identify and remove any "external" elements, such as "bugs". Moreover, in case of a disaster as stated in the previous paragraph, proper labeling and documentation could speed up the repair time.

Protecting our equipment is not enough. As we will see, our trash needs also protection and proper ways of disposal. Hackers or other persons trying to get access to our network often use the so called "dumpster diving" technique which can give them valuable information about our security protocols, anti hacking measures, the topology of our network and possible soft spots in security or in the infrastructure, or even worse give them access codes and usernames which can lead them directly into our network. The technique is carried out by just inspecting our trash hoping to find valuable data. It is thus of great importance to destroy all sensitive data before disposal and not just leave them in the dumpster as an easy prey for anyone to find.

4. Conclusions

Checking the proper operation and ensuring the safety of PBX as well as protection against unauthorized use and access is usually left to the owner. This has of course tremendous effects since due to economic and technical difficulties, in essence it is impossible to guarantee that the proper measures are taken. Avaya's PBX user manual states that it is impossible to guarantee 100% security since the owner has the final word in setup and administration of the switch and as so every unauthorized use claims are charged to the owner. Finally, FCC and courts both agree that the owner bears the responsibility for misuse of his system and not the manufacturer.

With the advent of new telecommunication technologies which are based around open communications via the Internet Protocol (VoIP) the situation will get even more complicated [14]. The introduction of these technologies means that IT and telecoms managers need now to become even more alerted to prevent new and existing threats that are typically associated with data networks, now impacting voice networks. Conventional PBXs typically use proprietary protocols and specialized software and have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers are multiplied [8]. Without diligent attention, telecoms systems are in grave danger of becoming the weak link in the network and utterly defenseless against targeted attacks.

PBX fraud has been allowed to flourish due to ignorance and naivety. Telephony security has remained a poor second place to IT security [3]. Hopefully this simple taxonomy with the comical perspective of things and the headlines that come with the illustration will help to better understand the dangers and the problems and will always be a good quick reference guide for the administrators. After all, it is not a matter of if… it is a matter of when!

References:

[1] Craig Pollard, "Telecom fraud: the cost of doing nothing just went up, White paper", Insight Consulting, Feb 2005.

[2] David West, "De-Mystifying Telecom Fraud", Telecom Business, July 2000.

[3] Vincent Blake, "PABX Security, Information Security Technical Report", vol. 5, no. 2. (2000) pp. 34-42.

[4] Kevin D. Mitnick and William L. Simon, "The Art of Deception: Controlling the Human Element of Security", Willey Publishing, Inc., 2002.

[5] Archer, White, et al. "Voice and Data Security", Sams Publishing, Indianapolis, Indiana, 2001.

[6] Dorothy E. Denning, "Information warfare and security", Addison-Wesley Professional, 1st edition, 1998.

[7] Iosif Androulidakis, "PBX security", 2nd Pan-Hellenic Conference on Electronic Crime, Athens 23-26/11/2004.

[8] Walsh, T.J.; Kuhn, D.R., "Challenges in securing voice over IP", IEEE
Security & Privacy, vol. 3, no. 3, May-June 2005, pp. 44-49.

[9] Wikipedia, Pbx, http://en.wikipedia.org/wiki/Pbx, March 2007.

[10] Avaya Inc, "Avaya Products Security Handbook", Issue 8, Nov 2002, Chapt. 2.

[11] Wade H. Baker and Linda Wallace, "Is information security under control?", IEEE Security & Privacy, vol. 5, no. 1, pp 36-44

[12] NIST , "PBX vulnerability analysis", special publication 800-24, 2001

[13] Jorge A. Ruiz-Vanoye et al, Strategy Planning for the computer science security, WSEAS Transactions on Computers, Issue 5, Vol 7, 2008, pp 387-396

[14] Jose-Vicente Aguirre et al, Secure VoIP and instant messaging on small PDA devices, WSEAS Transactions on Computers, Issue 1, Vol 5, 2006, 171-176

[15] Sanjay R. Ganorkar, Iris Recognition: An Emerging Biometric Technology, Proceedings of 6th WSEAS International Conference on Signal Processing, Robotics and Automation, 2007, pp 91-96

[16] Communications Fraud Control Association (CFCA), Worldwide Telecom Fraud Survey, CFCA, March 2003

[17] SecureLogix Corporation, White paper: Voice Network Management Best Practices, March 2007